Proficient preserve of changing password using android mobile

[1]G.N.Prabhakar, [2]R.Rajasekar
[1] B.Tech student, [2]Assistant Professor
[1,2]Department of Information Technology, SKP Engineering College, Tiruvannamalai , Tamilnadu.
[1]prabakar888@gmail.com , [2]Rajasekar.sept@skpec.in

Abstract - **All the company employee have some unique username and password .If colleague anyone know username and password of others means ,there is chance to leak out our company details and important document .so we have to avoid that. If hackers any one can type username and password in pc without permission means the intimation msg will be sent to authorized mobile. At the same time the authorized person will logout and change their password of unique id through mobile .so the unauthorized person will not able to take the file or document .The unique id will logout and next time hacker will not able to access the account**

Index Terms: **Unique id, hacker, and colleague**

I.INTRODUCTION

Most of the organization using remote monitoring using from computer to computer only. It is helpful to watching the employee performance during working hour .All the employees having username and password individually. Now we are implementing the concept change the password of pc with the help of mobile .Suppose the employee dint sign out their account means using android mobile authorized persons will logout the account while hacker's using others password. Before changing password proprietor of the unique id can get intimation message. First are ways in which mobile messaging has been structured by the power geometries of existing places of home, company, and public places. But also by youths' position in historically specific social structures. Mobile messaging provides a mechanism through which youth can overcome some of the adult-controlled power structures that govern their everyday lives.

II. PROPOSED METHODOLOGY

In proposed system we have to log out the page of admin login page using android mobile by having intimation message through computer to android mobile using web services .automatically admin login page of hacked is log out and changing password.

a. Employee registration:

Employee will sign up for using mail purpose which is used inside the company. The data are stored in my sql database as backend and frontend is php. We are using first name, last name, password, mobile number, address, favorites .this can be used to create the employee mail id uniquely or individually. **Employee recommendation** is an internal enrollment method employed by organizations to recognize potential candidates from their existing employees' social networks. An employee recommendation method encourages a company's existing employees to choose and engage the appropriate candidates from their social networks. As a accolade, the employer typically pays the referring worker a referral bonus. Recruiting candidates using employee recommendation is widely acknowledged as being the majority price effective and competent recruitment method to recruit candidates and as such, manager of every sizes, across all industries are trying to enlarge the volume of recruits through this waterway. Proponents of employee recommendation schemes allege the benefits to be an improved candidate excellence, 'fit', and preservation levels, while at the same time delivering a significant decline in recruitment disbursement. However, there are a number of potential drawbacks. One of the utmost concerns tends to be that relying too heavily on employee referrals could perimeter diversity in the administrative center, with new employees recruited in the similarity of existing employees. But, provided that there is previously a diverse workforce in position this ceases to be such an matter.

b. Login process:

User can use their signup username and password in the login page. This will check the database which is stored in mysql. If password is wrong means the sign in page will automatically logout . if it is correct means log in successfully. A personal identification number (PIN, pronounced "pin"; often erroneously PIN number) is a numeric password shared between a user and a system that can be used to authenticate the user to the system. Naturally, the user is required to provide a non-private user identifier or token (the user ID) and a confidential PIN to gain access to the system. Upon retrieve the user ID and PIN, the system monitoring the PIN based upon the user ID and compares the seeing PIN with the received PIN. The user is decided access only when the number entered matches with the number stored in the system. Hence, in spite of the name, a PIN does not personally identify the user.

EXPERIMENTAL SETUP:

a. Architecture diagram:

In this architecture diagram we are clearly identify the process of this project ideas completely. whenever login by user of owner corresponding data are gives request to admin .admin will check the data base and give response to admin .Automatically the intimation message will send to user of owner .he is able log out the login page of computer login page hacked by hacker and able to change the user name and password through mobile itself

Example Scenario for explaining the architecture fully

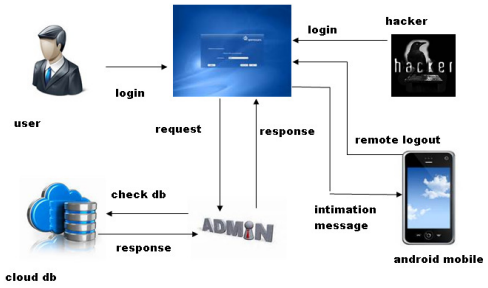

Figure 1:System Architecture

b. Intimation:

Intimation process which is using java programming for sending intimation message to mobile from pc whenever sign in login page. This intimation will help us to know the details about timing of login. At the same time the authenticated mail id person will able to log out his/her login page through the mobile .this process of logout will helps to logout the mail login page which is opened by hacker in pc. As more and more employee world wide attain and use mobile phones, so are they engross themselves in text messaging. Such is the situation that some hackers , themselves are expressing concerns that owner email id skills stand the risk of being sacrificed on the altar of text messaging. The occurrence has brought in its awaken three major organization of thought. While some employee think that text messaging is one of the banes of mobile telephony because of its possible negative impact on security skills of owner of id ;others contend that it rather enhances their security skills, and therefore is a blessing. A third group thinks that the argument is neither here nor there – text messaging has positive impact on security purpose . The first concision, and economy, the simple message system (SMS) of text messaging throws the essential mechanics of owner for security.

Figure 2:Intimation

III. CLOUD SERVER

A cloud server is different from a regular server. because the resources on the cloud server such as computing power and data storage space used more efficiently. And cloud server is dynamic private virtual server and it is partitioned such that it emerges as several servers. Cloud server is a virtual machine that acts in place of the normal physical server. It can be booted independently at the same time user operating system. The advancement in technology has eradicated the distances and enhanced the technological advent towards cloud server. The cloud also focuses on maximizing the effectiveness of the communal resources. Cloud resources are typically not only shared by multiple users but are also dynamically reallocated per insist. This can work for allocating capital to users. For example, a cloud computer ability that serves European users during European commerce hours with a specific function (e.g., email) may transfer the same resources to hand out North American users during North America's business hours with a diverse application (e.g., a web server). This approach should capitalize on the use of computing power thus reducing environmental smash up as well since fewer power, air conditioning, rack space, etc. are required for a variety of function. With cloud computing, multiple users can right of entry a single server to reclaim and update their data without purchasing licenses for different applications.

IV. SPAM FILTER

Spam filter can be filter on the company and unwanted messages that cannot be stored in ordinary database. A spam filter is a program that is used to detect unsolicited and unwanted email and prevent those messages from getting to a user's store box. Like other types of filtering programs, a spam filter looks for certain module on which it basic judgments. For example, the simplest and earliest versions (such as the one available with Microsoft's Hotmail) can be set to watch for particular words in the subject line of messages and to exclude these from the user's store box. This method is not especially energetic, too often exception perfectly legitimate messages (these are called false positives) and getting actual spam through. Web spam refers to a mass of techniques to challenge the ranking algorithms of web search engines and cause them to rank search outcome advanced than they would or else. example of such techniques comprise content spam and cloak (serving different versions of a page to search engine

Figure 3:Spam Filter

crawlers than to human users). Web spam is irritating to search engine users and unsettling to search engines; as a result, most viable search engines try to struggle web spam. Combating web spam consists of identifying spam content with high likelihood and – depending on policy – reduction it during ranking, eliminating it from the file, no longer swarming it, and tainting joined content. The first step – identifying probable spam pages – is a classification difficulty willing to machine education techniques. Spam classifiers take a large set of diverse features as input, including content-based features, link-based features, DNS and domain-registration facial appearance, and understood user feedback. profitable search engines treat their precise set of spam-prediction features as tremendously proprietary, and features (as well as spamming techniques) evolve continuously as search engines and web spammers are occupied in a continuing "arms race". Content spam refers to any web spam method that tries to look up the probability that a page is return as a search consequence and to get better its ranking by populating the page with most important keywords. Populating a page with words that are accepted query conditions will cause that page to be fraction of the result set for those question; choosing good combinations of query conditions will augment the portion of the bearing score that is based on textual facial appearance. Inexperienced spammers might carry out content spam by stringing together a extensive array of popular query terms. Search engines can defy this by employing language modeling techniques, since web pages that surround many topically unconnected keywords or that are grammatically ill-formed will reveal statistical differences from normal web pages .More complicated spammers might spawn not a hardly any but rather millions of end web pages, each page augmented with just one or a few popular query stipulations. The remainder of the page may be entirely machine-generated .

V. HACKER

In the computer security context, a hacker is someone who search and expect weaknesses in a computer system or computer network. Hackers may be encouraged by a huge number of reasons, such as profit, protest, or challenge. The nature, that has evolve around hackers is often get information to as the computer underground and is now a known community. Whenever other uses of the word hacker exist that are not related to computer security, such as referring to someone with an superior understanding of computers and computer networks, they are rarely used in typical context. They are subject to the time-honored hacker meaning controversy about the true meaning of the term hacker.

Figure 4 :Hacking

VI.SECURITY

Analyze the necessary security for the company, the staff, the resources, the products and the know how. Know about the motivation and plans of e.g. thieves, hackers, irritated employees, organized offense, violent pressure groups, and extremists. Local security negotiator should be asked to provide initial information and preserve a reporting system. Make sure that a security analysis is a original aspect of the overall business stability planning and decisions on all initial expenditures and investments. Determine what is satisfactory and what is not .It is significant to understand how technical, workforce and managerial means of security act together and help to protected other processes. Make sure that employees, provider and service provider are aware of, and respect the company's security rules and procedures. This information should be a essential part of the "day one" package for new employees and contactors but also for e.g. visitors, possibly in a shortened version. Communications, conversation and information exchanges between stakeholders such as employees, communities, clients, dealer, examine provider and government officials and agencies profile which is maintained in the company database, balanced with safeguards for sensitive information.

By the chance this details can be stole and issued to some other company by hacker .so remote monitoring logout method will be helpful to secure the mailing technique in any one organization.

VIII. CONCLUSION AND FUTURE WORK

In every organization each employee have some unique username and password .If colleague any one know username and password of others means ,there is chance to leak out our company details and important document .so we have to avoid that. The front end page is done by php and backend is mysql. This can be used to get the intimation message to correct user id person mobile, while whenever unauthorized person access another login. At the same time correct user id owner of the person will able to logout and change their password of unique id through mobile .this mobile logout process will automatically log out the pc login page .so the unauthorized person will not able to take the file or document .The unique id will logout and next time hacker will not able to access the account . This project will done by us.In future we are able to retrieve the IP address when the hackers login with others login username and password..It will show the correct computer where the hacker use the corresponding pc.

REFERENCES

[1] M. Arm brust et al., “Above the Clouds: A Berkeley View of Cloud Computing,” technical report, Univ. of California, Berkeley
[2] V.Kundra, “Federal Cloud Computing Strategy”,
[3] Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing.
[4] S. Subashini and V. Kavitha, "A survey on security issues in service Delivery models of cloud computing", Journal of Network and Computer Applications
[5] I. Burguera, U. Zurutuza and S. Nadjm-Tehrani, "Crowdroid: behavior based The fitting detection system for android", Proceedings of the 1st workshop on Security and privacy in smart phones and mobile devices.